UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/625,363	07/23/2003	Ramarathnam Venkatesan	MS1-1285US	8229

22801 7590 08/23/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
GEE, JASON KAI YIN

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/625,363	**Applicant(s)** VENKATESAN ET AL.	
	Examiner Jason K. Gee	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 20 June 2007.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 and 26-38 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 and 26-38 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is response to communication: amendment filed on 06/20/2007.

2. Claims 1-20 and 26-38 are currently pending in this application. Claims 21-25 and 39-43 have been withdrawn. Claims 1, 12 and 26 are independent claims.

3. No new IDS has been received since the previous Office Action

Response to Arguments

4. As per claims 2-11 and 13-25, the appellant has argued that "A medium as recited in claim…" is proper. However, the Examiner still believes the term "a" should be changed to "the" to distinctly point to the medium as recited in claim 1.

5. As per claims 11, 20, 28, 29, 37, and 38, the applicants argue that the claims are dependent claims. In response to applicant's arguments, these claims are considered dependent claims.

6. In regards to the art rejections, the Pintsov reference still stands for the rejections that do not add the limitations of the equations. The limitation "and M2 cannot be derived form these calculations of one or more codes" is still taught in the Pintsov reference, as seen in the art rejection below. In regards to the claims that add additional limitations incorporating a specific equation, another reference is now brought in, and the arguments regarding those rejections are now moot in light of new references.

Claim Objections

7. Claims 2-11, 13-25, and 27-38 are objected to because of the following informalities:

As per claims 2-11 and 13-25, the claims recite "A medium as recited in claim ..." However, this should be changed to "The medium as recited in claim ..." to distinctly specify the medium as described in the claims in which they are dependent on. Appropriate correction is required.

In regards to claims 27-38, the claims have been amended to recite that they are dependent on claim 1, and not claim 26, as originally claimed. However, the Examiner believes that this is a typographical error, as the status of the claims have not been changed (still Original, not Amended). The appellant is required to address this discrepency in the next reply. If the applicants did intend for this amendment, the status of the claims are not correct, and this amendment is non-compliant. Further, if this is indeed an amendment, many 101 and 112 issues will arise.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 11-20 and 26-38 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per these claims, the independent claims have been amended to recite "and M2 cannot be derived from these calculations of one or more codes." However, this is a negative limitation that has not been described explicitly in the specification.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-4, 7, and 10 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Pointsov European Patent Application EP 1083700 A2 (03/14/2001).

As per claim 1, Pintsove teaches a computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising: obtaining a message M having two portions, wherein M1 is one of the portions of the M and M2 is another (paragraph 8, wherein M2 is the hidden first portion, and M1 is the visible second portion); generating one or more codes having a combination with M2 implicitly embedded therein, wherein calculations that generate the one or more codes do not employ M2, and M2 cannot be derived from these calculations of one or more codes (paragraphs 8 and 19-24, wherein codes are generated using c; also see paragraph 23, wherein the final signature is created utilizing s,c, and v; further M2 cannot be derived from C, as a hash function is used (paragraph 20, wherein a hash function is always one-way)); reporting the one or more codes, by which reporting the one or more codes facilitates a cryptographic technique for protecting digital media (paragraphs 23-24, wherein s, c, and v are reported to form a signature).

As per claim 2, Pintsove teaches wherein the method further comprises producing a digital signature (DS) comprising M1 and the reported one or more codes (paragraph 8 and 23).

As per claim 3, Pintsove teaches wherein two or more codes are generated by the generated and reported by the reporting (paragraph 8, wherein one code is the first component, and the second code is the second component; also detailed in paragraphs 19-24).

As per claim 4, Pintsove teaches wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code (paragraph 8, 20, 21; Figure 1).

As per claim 7, Pintsove teaches wherein the generating comprises: finding a value of a variable per-message key (k) where a predefined mathematical function employing k produces a result equivalent to M2 (paragraphs 19-25, and 29); when such a value of k is found, calculing the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k (paragraphs 19-25, and 29).

As per claim 10, Pintsove teaches wherein the method further comprises producing a digital signature (DS) comprising M1 and the reported codes r and s (paragraphs 8 and 29, wherein the signature is (s, c, V).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 7-9, 11-14, 17-20, 26-28, 30, 33, 34, 36, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable Pintsov as above, and further in view of Venkatesan et al. US Patent No. 6,209,093 (hereinafter Venkatesan)..

As per claim 7, Pintsov, as understood by the Examiner, does not explicitly teach all the limitations of this claim. Pintsove teaches though utilizing ElGamal equations though in paragraph 23, which utilize similar equations. However, this formula is not explicitly shown in Pintsove. However, this is shown in Venkatesan, such as in col. 13 lines 10-15.

At the time of the invention, it would have been obvious to combine the teachings of Venkatesan with Pintsov. One of ordinary skill in the art would have been motivated to perform such an addition to increase security. Although the equation shown in Venkatesan are slightly different (the r instead of M2), it would have been obvious to modify this equation to apply in this scenario, as it increases security. Further, Venkatesan is analogous art, as it is directed toward cryptographic signatures and authentication.

Claim 8 is rejected using the same basis of arguments used to reject claim 7. Non-linear mathematical functions are taught throughout Pintsove, such as in paragraphs 14 and 29, wherein DES and SHA both employ non-linear mathematical functions. Further, more details can be found in Venkatesan col. 12 line 42 to col. 13 line 20.

As per claim 9, Pintsove teaches finding a value of a variable per-message key (k) where a predefined mathematical function employing M1 and g^k produces a result equivalent to M2 (paragraphs 19-25, and 29); when such a value of k is found, calculating the two or more codes, where one code is r (paragraphs 19-25, and 29, where r is c) and another is s (paragraphs 19-25, and 29, where s is s), with r (c) being calculated using another predefined mathematical function employing M1 and g^k (paragraphs 19-25, and 29), and with s being calculated using still another predefined mathematical function employing M1, and g^k and r (paragraphs 19-25, and 29, wherein s = k-1 {SHA1(c//V)+a r'} modn. Further, details utilizing k is taught in Venkatesan such as in col. 12 line 42 to col. 13 line 20. Here, k is utilized in more equations.

Claim 11 is rejected using the same basis of arguments used to reject claim 1. A peripheral device is taught in Venkatesan in col. 6 lines 5-15.

Independent claim 12 is rejected using the same basis of arguments used to reject claims 8 and 9.

Claim 13 is rejected using the same basis of arguments used to reject claim 10.

Claim 14 is rejected using the same basis of arguments used to reject claim 8.

Claim 17 is rejected using the same basis of arguments used to reject claim 9 above.

Claim 18 is rejected using the same basis of arguments used to reject claim 8 above.

Claim 19 is rejected using the same basis of arguments used to reject claim 10 above.

Claim 20 is rejected using the same basis of arguments used to reject claim 11 above.

Independent claim 26 is rejected using the same basis of arguments used to reject claim 12 above.

Claim 27 is rejected using the same basis of arguments used to reject claim 13 above.

As per claim 28, Pointsov teaches a digital signature created throughout the reference. As the digital signature is created on a computer, as taught throughout the reference, it would be inherent that the digital signature is stored on a computer-readable medium, at least temporarily. The other limitations of the claims are rejected using the same basis of arguments used to reject claim 27.

Claim 30 is rejected using the same basis of arguments used to reject claim 14.

Claim 33 is rejected using the same basis of arguments used to reject claim 17. Further, since none of the variables are actually defined (except M1), any art teaching a mathematical function employing the message M1 would meet these limitations.

Claim 34 is rejected using the same basis of arguments used to reject claim 18.

Claim 36 is rejected using the same basis of arguments used to reject claim 19, wherein a message is a digital signature.

As per claim 37, it is inherent to the teachings of Pintsov that a computer-readable medium embodies a message, as the processes of Pintsov require a computer.

14. Claims 5, 6, are rejected under 35 U.S.C. 103(a) as being obvious over Pintsov European Patent Application Ep 1083700 A2 (hereinafter Pintsov).

As per claim 5, Pintsov teaches wherein the message M has a defined length (paragraph 9, wherein M1 and M2 (the combination of M1 and M2 make up M) have a determined length). However, at the time of the invention, Pintsov does not explicitly teach wherein the length of the combination of the two or more codes is less than the message's defined length. Pintsov teaches though that the two codes are hashed though in paragraph 8 and throughout the reference. It is well known in the art that hashing reduces the data into a small number that serves as a fingerprint. If both the codes were hashed to less than half the size, it would be true that the length of a combination of two or more codes is less than the message's defined length.

At the time of the invention, it would have been obvious to have the length of a combination of two or more codes to be less than the message's defined length. One of ordinary skill in the art would have been motivated to perform such an addition to increase the speed of the whole process and a better flow of data by having codes that are smaller than half the size of the original message.

As per claim 6, Pintsov teaches wherein M2 has a defined length (paragraph 9, wherein M2, the first portion, has a size determined by an application). However, at the time of the invention, Pintsov does not explicitly teach wherein the length of the combination of the two or more codes is less than the defined length of M2. Pintsov teaches though that the two codes are hashed in paragraph 8 and throughout the reference. It is well known in the art that hashing reduces the data into a small number that serves as a fingerprint. If both the codes were hashed to less than half the size, it would be true that the length of a combination of two or more codes is less than M2's defined length.

At the time of the invention, it would have been obvious to have the length of a combination of two or more codes to be less than M2's defined length. One of ordinary skill in the art would have been motivated to perform such an addition to increase the speed of the whole process and a better flow of data by having codes that are smaller than half the size of the original message.

15. Claims 15, 16, 29, 31, 32 35, and 38 are rejected under 35 U.S.C. 103(a) as being obvious over Pintsov European Patent Application Ep 1083700 A2 (hereinafter Pintsov) in view of Venkatesan.

Claim 15 is rejected using the same basis of arguments used to reject clam 5 above.

Claim 16 is rejected using the same basis of arguments used to reject claim 6 above.

As per claim 29, Pointsov does not explicitly teach wherein a digital signature is embodied as human-readable indicia on a human readable medium. However, a digital signature embodied as human-readable indicia on a human-readable medium is well known in the art and it would have been obvious to do so. One of ordinary skill in the art would have been motivated to perform such an addition as to be able to provide a digital signature so that humans can be able to see it and confirm the signature visually. Also, providing a signature that can be confirmed visually would be practical and would require less calculations. The remaining limitations of the claims are rejected using the same basis of arguments used to reject claim 27 above.

Claim 31 is rejected using the same basis of arguments used to reject claim 5 above.

Claim 32 is rejected using the same basis of arguments used to reject claim 6 above.

As per claim 35, Pointsov teaches all the limitations of the claims, but does not explicitly teach wherein the predefined mathematical function for is quadratic. As can be seen in the rejection for claim 34, Pointsov teaches that the predefined mathematical function for s is non-linear. However, a quadratic equation is well known in the art, and would be obvious to implement. At the time of the invention, it would have been obvious to one of ordinary skill in the art to include a quadratic as the mathematical function for s. Quadratics are well known in the art, and easy to solve, and it would have been obvious to include a quadratic equation as a non-linear equation.

Claim 38 is rejected using the same basis of arguments used to reject claim 29 and 36 above, wherein a digital signature is a type of a message.

Conclusion

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
08/07/2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER